IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	C. A. No. 04-1199 (SLR) **REDACTED**

SRI INTERNATIONAL, INC.'S OPENING BRIEF IN SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT OF NO ANTICIPATION BY THE "EMERALD 1997" PUBLICATION

Dated: June 16, 2006

FISH & RICHARDSON P.C.

John F. Horvath (#4557)
FISH & RICHARDSON P.C.
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
FISH & RICHARDSON P.C.
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff and Counterclaim Defendant
SRI INTERNATIONAL, INC.

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. NATURE AND STAGE OF THE PROCEEDINGS 2

III. STATEMENT OF FACTS 2

IV. ANALYSIS 5

A. Legal standards 5

B. EMERALD 1997 does not explicitly or inherently disclose the required types of network traffic data 6

1. Analyzing firewall logs does not necessarily require monitoring and analyzing the network traffic data of the Markush groups 7

2. Analyzing SNMP traffic does not necessarily require monitoring and analyzing the network traffic data of the Markush groups 9

3. The nature of the intrusion attacks does not naturally lead to monitoring the types of network traffic data required by the Markush groups 10

4. Sniffers do not necessarily monitor and analyze the types of network traffic data required by the Markush groups 11

5. Defendants' obviousness arguments underscore the lack of inherent anticipation by EMERALD 1997 12

V. CONCLUSION 14

TABLE OF AUTHORITIES

Page(s)

Cases

Akamai Techs., Inc. v. Cable & Wireless Internet Services, Inc.,
344 F.3d 1186 (Fed. Cir. 2003) 6, 7, 9

Celotex Corp. v. Catrett,
477 U.S. 317 (1986) 6

Connell v. Sears Roebuck & Co.,
722 F.2d 1542 (Fed. Cir. 1983) 5

Invitrogen Corp. v. Biocrest Mfg., L.P.,
424 F.3d 1374 (Fed. Cir. 2005) 5

Metabolite Labs., Inc. v. Lab. Corp. of America Holdings,
370 F.3d 1354 (Fed. Cir. 2004) 6, 14

Minn. Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.,
976 F.2d 1559 (Fed. Cir. 1992) 6

Perricone v. Medicis Pharm. Corp.,
432 F.3d 1368 (Fed. Cir. 2005) 6

Telemac Cellular Corp. v. Topp Telecom.,
247 F. 3d 1316 (Fed. Cir. 2001) 10

Toro Co. v. Deere & Co.,
355 F.3d 1313 (Fed. Cir. 2004) 6

Statutes

FED. R. CIV. P. 56(c) 6, 14

I. INTRODUCTION

Although they concede that EMERALD 1997, a prior art reference authored by one of the inventors of the patents-in-suit and cited to the Examiner during the prosecution of the patents, does not expressly anticipate any of the claims at issue in this litigation, Defendants assert that the reference *inherently* anticipates certain claims of the '338, '615 and '203 patents. To prevail on a claim of inherent anticipation, Defendants must prove by clear and convincing evidence that EMERALD 1997 *necessarily* includes every limitation that is not expressly disclosed. Since each of the claims asserted to be anticipated by EMERALD 1997 requires analysis of particular types of network traffic data as recited by the claims' Markush groups, and since EMERALD 1997 does not necessarily disclose the analysis of those types of network traffic data, Defendants cannot carry their burden of establishing inherent anticipation and SRI's motion must be granted.

EMERALD 1997 is an early, overview paper that describes SRI's proposed research program aimed at developing a practicable and scalable architecture for identifying intrusions in large-scale enterprise networks. This paper was written by one of the inventors of the patents-in-suit, Philip Porras, shortly after he joined SRI and began the research that ultimately lead to the conception and reduction to practice of the claimed inventions.

As part of a generalized description of potential avenues of research that SRI intended to pursue, EMERALD 1997 identifies a number of possible data sources to explore that might be useful in tackling the intrusion detection problems outlined in the paper. Disclosure of these generic data sources, however, does not automatically or necessarily lead one of ordinary skill in the art to create a system that selectively monitors and analyzes the particular types of network traffic data (as opposed to all traffic or other, non-claimed data types) that are expressly required by the asserted claims. Only by making a series of complex design choices, on which EMERALD 1997 provides no guidance, could one create a system that monitors the claimed types of

network traffic data. As a matter of law, the fact that the creation of such a system involves any design choice at all precludes EMERALD 1997 from inherently anticipating the claims.

II. NATURE AND STAGE OF THE PROCEEDINGS

SRI International, Inc. ("SRI") sued Internet Security Systems, Inc., a Delaware corporation, Internet Security Systems, Inc., a Georgia corporation (collectively, "ISS"), and Symantec Corporation ("Symantec") for infringing U.S. Patent Nos. 6,321,338 ("the '338 patent") [Ex. A[1]], 6,484,203 ("the '203 patent") [Ex. B], 6,711,615 ("the '615 patent") [Ex. C], and 6,708,212 ("the '212 patent") [Ex. D] (collectively, "the patents-in-suit"). All discovery relevant to the first trial on liability is complete. The parties have exchanged expert reports and have submitted their opening briefs on claim construction. Claim construction and summary judgment hearings are scheduled for August 23, 2006.

III. STATEMENT OF FACTS

The patents-in-suit are the result of SRI's EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) series of research projects. Early in this research, one of the named inventors, Phillip Porras, submitted an article for possible future publication which provided a high-level overview of the then-planned architecture of EMERALD. [Ex. E at 440:11-12; Ex. F at ¶22]. This early conceptual overview of the project was eventually published in October 1997. [Ex. G]. As the inventions described and claimed in the patents-in-suit stem from the EMERALD research project, EMERALD 1997 was cited to the Examiner during their prosecution. [Exs. A-D at p. 2]. Having considered EMERALD 1997 and a host of other cited references (including others related to EMERALD itself), the Examiner allowed all the claims of the patents-in-suit in first action allowances.

[1] All referenced exhibits are attached to the Declaration of Kyle Wagner Compton.

Despite the Examiner's decision otherwise, Defendants now allege that EMERALD 1997 anticipates many of the asserted claims, including the following:

- claims 1-6, 8, 10-19, 21, 23, 24, and 25 of the '338 patent (all of which require, among other things, detecting suspicious activity through measures of network packets, at least one measure monitoring data transfers, errors, or network connections);
- claims 1-23, 38, 48, 68, and 88 of the '615 patent (all of which require detecting suspicious network activity based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols}); and
- claims 1-22 of the '203 patent (all of which require detecting suspicious network activity based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}).

[Ex. H at ¶258; Ex. I; Ex. K]. All of these claims require monitoring or analysis of selected types of network traffic data, as opposed to all network traffic data. Selective filtering of the abundance of information contained in the entirety of the available network traffic data is critical to creating a system that can practically scale to an enterprise network. [Ex. F at ¶¶13, 14]. The selection of the particular subset of data to focus the analysis on, in order to obtain a workable system for detecting intrusions, was far from trivial at the time of the effective filing date of these patents. Defendants allege, however, that monitoring and analysis of the specific types of network traffic data

required by the Markush groups of the above claims is *inherently* disclosed in EMERALD 1997. [Ex. L at ¶¶13, 59, 60, 80; Ex. H at ¶¶252-255; Ex. J at 29-31].

In their attempt to find inherent disclosure of analysis of the required types of network traffic data, Symantec's experts focus on a portion of EMERALD 1997 that describes a variety of possible sources of data to explore analyzing to detect intrusions:

> "Underlying the deployment of an EMERALD monitor is the selection of a target specific event stream. The event stream may be derived from a variety of sources including audit data, network datagrams, SNMP traffic, application logs, and analysis results from other intrusion detection instrumentation."

[Ex. G at ISS02895; Ex. L at ¶¶44, 49, 80; Ex. F at ¶¶252, 253]. This statement merely identified potential, generalized data sources, several of which (*e.g.*, audit data) are not necessarily even network traffic data at all. [*See e.g.*, Ex. H at ¶91 (explaining audit trails)]. EMERALD 1997 does not, however, provide any specific guidance as to which data source to use or how to select between the various types of information that are contained within each general source.

Symantec's experts, Fredrick Avolio and Todd Heberlein, opine that by disclosing the possibility of monitoring "application logs," EMERALD 1997 inherently discloses analysis of the specific types of network traffic required by the Markush groups of the '338, '615, and '203 claims. [*e.g.*, Ex. L at ¶¶13, 59, 60, 62, 63, 66, 67, 68; Ex. H at ¶252 (adopting Mr. Avolio's Report)]. Their allegations can be summarized as follows: (1) EMERALD 1997 discloses monitoring a network by selection of a target specific event stream, which *might* be derived from an application log [Ex. L at ¶49, 80]; (2) the application log *might* be a firewall log [*id.* at ¶¶50, 54]; (3) [*some*] firewalls known in 1997 *might be configured* to monitor packet data volume or network connection requests and denials [*id.* at ¶ 13]; therefore (4) EMERALD 1997 allegedly *necessarily* discloses monitoring and analyzing packet data volume and network connection requests and denials. [*Id.* at ¶¶13, 60, 80].

When deposed, Mr. Avolio confirmed that an application log is not necessarily a firewall log. [Ex. M at 64:17-65:2]. Mr. Avolio also admitted that not all firewalls known in 1998 had logging capabilities [*id.* at 42:23-25; 43:3-4] and that "thought and analysis" was required to determine what data a firewall should be configured to log in a given environment. [*Id.* at 71:23-72:3].

In addition to the alleged inherent disclosure based on firewall logs, Mr. Heberlein alleges that the required types of network traffic are also inherently disclosed because "EMERALD 1997 disclosed monitoring an event stream of SNMP traffic and monitoring network infrastructure" and "SNMP traffic and related network infrastructure management data provides monitoring for a *variety of different categories* of network traffic data." [Ex. H at ¶253(emphasis added)]. Mr. Heberlein also suggests that the types of network traffic data are inherent as they allegedly "flow naturally from the types of attacks." [*Id.* at ¶254-255].

Mr. Smaha, ISS's expert, takes a different and more cursory route to allegedly find inherent disclosure of the required types of network traffic data. The entirety of the discussion on the topic in his expert report states: "Inherent in the use of these network packet capture and analysis routines are the examination of network packet data transfers commands, volume, errors, requests, and denials." [Ex. J at 31].

IV. ANALYSIS

A. Legal standards

An issued patent is presumed to be valid. 35 U.S.C. § 282 (2000). A party attempting to demonstrate invalidity must do so by clear and convincing evidence. *Connell v. Sears Roebuck & Co.*, 722 F.2d 1542, 1549 (Fed. Cir. 1983). This same standard of proof also applies in the summary judgment context. *Invitrogen Corp. v. Biocrest Mfg., L.P.*, 424 F.3d 1374, 1378 (Fed. Cir. 2005). Summary judgment is appropriate when "the pleadings, depositions, answers to interrogatories, and admissions

on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." FED. R. CIV. P. 56(c); *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986).

To anticipate a claim, a single prior art reference must disclose every limitation of that claim. Limitations may be disclosed expressly or inherently. *Perricone v. Medicis Pharm. Corp.*, 432 F.3d 1368, 1375-1376 (Fed. Cir. 2005); *Minn. Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.*, 976 F.2d 1559, 1565 (Fed. Cir. 1992). A claim limitation will only be found to be inherently present when the prior art reference *necessarily* includes the limitation. *Akamai Techs., Inc. v. Cable & Wireless Internet Services, Inc.*, 344 F.3d 1186, 1192 (Fed. Cir. 2003). It is not sufficient that a limitation is merely *probably or possibly* present in the reference. *Id.* Thus, for inherent anticipation to be found, the prior art must sufficiently describe and enable at least one embodiment which necessarily includes the subject matter embraced by the particular claim limitation. *Toro Co. v. Deere & Co.*, 355 F.3d 1313, 1321 (Fed. Cir. 2004).

The party attempting to prove patent invalidity by inherent anticipation bears a "heavy burden," especially when the prior art was before the Patent and Trademark Office during prosecution. *Metabolite Labs., Inc. v. Lab. Corp. of America Holdings*, 370 F.3d 1354, 1368 (Fed. Cir. 2004). Defendants fail to come even close to meeting that heavy burden in this case.

B. EMERALD 1997 does not explicitly or inherently disclose the required types of network traffic data

EMERALD 1997 makes no explicit reference to any of the types of network traffic data recited in the Markush groups of the claims of the '338, '615, and '203 patents. Defendants recognize this and, therefore, resort to an allegation of inherent anticipation. [Ex. L at ¶59; Ex. H at ¶¶252-55; Ex. J at 31]. In order to prevail on the issue of inherent anticipation, Defendants must prove by clear and convincing evidence that EMERALD 1997 enables at least one embodiment which *necessarily* includes all the

limitations of the claims at issue. Put another way, Defendants must prove that a person of ordinary skill in the art at the time of filing, attempting to design a network intrusion detection method using only EMERALD 1997 as a guide, would *necessarily* construct a system which analyzes at least one type of network traffic data required by the Markush groups of the '615, '338, and '203 patents. *Akamai*, 344 F.3d at 1192 (Fed. Cir. 2003). Defendants cannot do so.

1. Analyzing firewall logs does not necessarily require monitoring and analyzing the network traffic data of the Markush groups

In his report, Mr. Avolio states: "although the *EMERALD 1997* reference does not recite verbatim the claimed network traffic data categories, several of these categories are necessarily present in the disclosure . . ." [Ex. L at ¶59]. Specifically Mr. Avolio alleges:

> "In configuring a firewall to conform to the requirements of the disclosed EMERALD monitoring system, . . . one would have necessarily analyzed multiple different claimed categories of network traffic data or measures of network packets, including: network connections (including both network connection requests and network connection denials), and data transfers (including network packet data volume)."

[*Id.* at ¶60]. In reaching this conclusion, Mr. Avolio appears to rely on a two step argument starting from the EMERALD 1997 disclosure that "[t]he event stream may be derived from a variety of sources including . . . application logs . . ." First, he states that: "One type of application log is a firewall log." [*Id.* at ¶50]. Second, he claims that: "Firewalls in 1997 monitored and logged: (1) network connections, including both network connection requests and denials, (2) data transfers, including network packet data volume and network packet data transfer volume." [*Id.* at ¶13]. Mr. Avolio's own report and deposition testimony, however, belie his own reasoning and inherent disclosure conclusion.

Consistent with his report, at his deposition, Mr. Avolio explained that "activity log" and "application log" are general terms, which may include firewall logs, but can also refer to logs of other types of activity and applications. [Ex. M at 64:12-25 and

65:1-2; Ex. L at ¶50]. Thus, Mr. Avolio acknowledges that an application log is not necessarily a firewall log. Rather, a firewall log is merely one possible type of application log, and a person of skill in the art, attempting to implement the disclosure of EMERALD 1997, would not necessarily create a system which analyzes firewall logs. To inherently disclose a limitation, however, it is not enough that a reference possibly disclose a claim element: it must necessarily disclose it.

Even assuming the term "application log" as disclosed in EMERALD 1997 was equated with "firewall log," it does not follow that the firewall log would necessarily include the particular data types required by the patents-in-suit. At the time of filing, the logging capabilities of firewalls varied considerably. Some firewalls did not even have logging capabilities. [Ex. M at 42:5-14; 42:23-25 and 43:3-4 (explaining that "certainly not all" firewalls that existed in 1998 had logging capability)]. For those firewalls that did include logging capability, many different types of data could be logged and users had to decide what types of data were practical and appropriate to log in their particular network environment. [Ex. M at 71:23-25; 72:1-3 (confirming that thought and analysis is needed to decide what data a firewall should log); *See also*, *Id.* at 71:1-8]. Out of the multiple possibilities, Defendants do not point to anything (other than the claims themselves) that would have led one of ordinary skill in the art to make the particular decisions that would lead to the claimed inventions. EMERALD 1997 provides no guidance as to what types of data, from a firewall or otherwise, would be practical and appropriate to log. Thus EMERALD 1997 does not necessarily disclose monitoring the particular types of network traffic data required by the claims at issue, and therefore cannot inherently disclose that limitation.

EMERALD 1997 instead presents one of ordinary skill with many potential sources of data to explore, by reciting "audit data, network datagrams, SNMP traffic, application logs, and analysis results from other intrusion-detection instrumentation." [Ex. G at ISS02895]. Even just focusing on application logs, one of ordinary skill would

have to make the design choice of what type of application log to use. Assuming selection of firewall logs, one of ordinary skill is then faced with yet another design choice – which firewall? Depending on the firewall selected, various different types of data could possibly be logged. The decision to then configure the selected firewall to monitor the particular data types required by the claims' Markush groups would be yet another design choice, not an inherent property of the firewall log. Given the many design choices identified by Defendants' own experts, the path from the disclosure in EMERALD 1997 to the creation of a system that selectively analyzes the particular types of network traffic data claimed in the '338, '615 and '203 patents is neither direct nor inevitable. As a consequence, EMERALD 1997 cannot inherently disclose this limitation. It is simply not sufficient that a reference possibly or even probably includes the limitation. *Akamai*, 344 F.3d at 1192 (Fed. Cir. 2003).

2. Analyzing SNMP traffic does not necessarily require monitoring and analyzing the network traffic data of the Markush groups

EMERALD 1997 discloses that "[u]nderlying the deployment of an EMERALD monitor is the selection of a target specific event stream. The event stream may be derived from a variety of sources including . . . SNMP traffic . . ." [Ex. G at ISS02895]. Mr. Heberlein explains that "SNMP traffic and related network infrastructure management data provides monitoring for a *variety of different categories of traffic data*." [Ex. H at ¶ 253 (emphasis added)]. The claims' Markush groups, however, require selective monitoring of particular types of network traffic data. Disclosing monitoring of a variety of different categories of traffic, which could *possibly* include some of those types of traffic data required by the claims, is legally insufficient to constitute inherent disclosure of them for the same reasons discussed above with respect to firewall logs. *Akamai*, 344 F.3d at 1192. EMERALD 1997 provides no guidance to one of ordinary skill in the art on how to distill SNMP traffic – which potentially contains

a variety of information for network management purposes – into a subset of network traffic data useful to detect intrusions. Nor does Mr. Heberlein even attempt to explain how or why, without the guidance of the claims, one of ordinary skill would necessarily make the specific design choices and decisions needed to produce the system recited in the claims, from the starting point of "SNMP traffic and related network infrastructure management data." The reason for the failure is clear; there is no principled basis, just a bare, unsupported conclusion. An unsupported conclusion, however, is insufficient to prevent summary judgment. *Telemac Cellular Corp. v. Topp Telecom.*, 247 F. 3d 1316, 1329 (Fed. Cir. 2001) ("Conclusory expert witness statements are not evidence and do not create a genuine issue of material fact.").

3. The nature of the intrusion attacks does not naturally lead to monitoring the types of network traffic data required by the Markush groups

As already discussed above with respect to firewalls and SNMP traffic, as of the time of the invention, a vast assortment of possible network traffic information could be monitored for a wide variety of purposes. EMERALD 1997, however, provides no guidance to one of ordinary skill in the art to select the specific types of network traffic data enumerated in the claims at issue for the purpose of detecting suspicious network activity. Indeed, the paper does not even limit its litany of potential data sources to network traffic alone, but includes within its discussion other potential sources of data. Even drawing upon one of ordinary skill in the art's limited knowledge of known attacks as suggested by Mr. Heberlein [Ex. H at ¶¶254-55], one of ordinary skill would not be led to *necessarily* select the types of network traffic data required by the claims. Attacks were varied and could be executed and manifested in numerous different ways. [Ex. F at ¶35]. There were also quite a number of prior art systems available at the time, including SRI's IDES and NIDES systems, that detected various attacks based on a completely different source of information – host audit logs. [*Id.* at ¶46; *See also* Ex. H at ¶¶91, 93,

104, 105]. References related to these and many other methodologies of intrusion detection were before the examiner along with the EMERALD 1997 paper and the claims were allowed without a single prior art rejection. The mere possibility – which Defendants' experts admit to be only that – that one of ordinary skill could have selected network "datagrams" as the input data source, and then honed in on the specific network traffic categories recited in the claims (after an undisclosed and unknown amount of time and experimentation) cannot as a matter of law support a conclusion that such subject matter is inherently disclosed in EMERALD 1997.

4. Sniffers do not necessarily monitor and analyze the types of network traffic data required by the Markush groups

The inherent disclosure analysis of ISS's expert, Mr. Smaha, is even more cursory and flawed than that of Symantec's experts. Mr. Smaha appears to point to EMERALD 1997's suggestion to explore using "datagrams" as data inputs and simply states: "Inherent in the use of these network packet capture and analysis routines are the examination of network packet data transfer commands, volume, errors, requests, and denials." [Ex. J at 31]. Mr. Smaha's reference to "network packet capture and analysis routines" is a reference to sniffers – products that capture network traffic – and that were relatively common in 1997. [*Id.* at 30-31]. In 1997, many types of sniffers were available. Like firewalls, these sniffers could monitor various types of network traffic, including categories of network traffic data not included within the claims of the patents-in-suit. EMERALD 1997, however, provides no guidance as to the specific types of network traffic data that *should be* monitored by these sniffers, as would be required to anticipate the claims at issue. Again, while it is *possible* that a sniffer could have monitored the specific types of network traffic data called out in the claims, it does not necessarily follow from the broad-brush conjectural disclosure of EMERALD 1997 that they do so. Therefore EMERALD 1997 cannot inherently disclose these types of network traffic data.

Mr. Smaha's citation in his expert report to the testimony of named inventor Phillip Porras provides no support for his conclusion that EMERALD 1997 inherently discloses the types of network traffic data enumerated in the claims at issue. [*Id.* at 31]. In response to the question

REDACTED

First, the question asked to Mr. Porras is not directed at the disclosure contained in EMERALD 1997 alone, but that disclosure in combination with the disclosure made at a presentation given by Mr. Porras. More importantly, however, Mr. Porras was asked whether it is *possible*, not whether it is *necessary* (as actually required by the law of inherent anticipation) that one would conclude that event streams must be derived from network packets. Additionally, the question only inquires about analysis of network packets generally, not the specific types of network traffic data actually required by the claims at issue. Again, far from supporting the conclusion that analysis of the claimed categories of network traffic was necessary, Defendants' argument at most supports the proposition that someone reading the EMERALD 1997 paper would conclude that analysis of such data was possible. Such a showing does not, as a matter of law, support a finding of inherency.

5. Defendants' obviousness arguments underscore the lack of inherent anticipation by EMERALD 1997

While Mr. Smaha contends that claim 1 of the '338 patent, which requires monitoring data transfers, errors, or network connections, is inherently anticipated, he does not contend that its dependent claims, which call out more specific types of network traffic data that fall within that Markush group, are inherently anticipated. He instead turns to obviousness arguments – combining (without motivation) EMERALD 1997 with various secondary references such as NetRanger or ISS RealSecure, which allegedly

disclose monitoring of the particular categories of network traffic data. [Ex. K]. Mr. Smaha provides no explanation for why his reasoning discussed above that sniffers monitor the enumerated traffic of the independent claim – data transfers, errors, or network connections – does not equally apply to data transfer commands (claim 2), network packet data transfer volume (claim 4), network connection requests (claim 5), or network connection denials (claim 6) as required by the dependent claims. [*Id.*]. In fact, his failure to assert inherent anticipation of these dependent claims contradicts the statement in his expert report that : "Inherent in the use of these network packet capture and analysis routines are the examination of *network packet data transfer* commands, *volume*, errors, *requests*, and *denials*." [Ex. J at 31]. Thus Mr. Smaha's obviousness arguments are an admission that the mere disclosure of using network sniffers does not necessitate monitoring any specific category of network traffic data enumerated in the independent or dependent claims at issue.

Mr. Smaha's reliance on secondary references such as NetRanger or ISS RealSecure, not EMERALD 1997, for disclosure of network packet data transfer volume (claim 4), network connection requests (claim 5), and network connection denials (claim 6) [Ex. K] also squarely contradicts the opinion of Messrs. Avolio and Heberlein that network connection requests, network connection denials, and network packet data volume are inherently disclosed in EMERALD 1997 itself. [Ex. L at ¶60]. Indeed, Mr. Heberlein apparently recognizes the weakness of his own allegation that monitoring specific types of traffic is inherently disclosed in EMERALD 1997, because he provides "alternative" obviousness arguments for all the claims requiring monitoring or analysis of specific types of network traffic. [Ex. I]. He looks to secondary references such as NetRanger, ISS RealSecure, and SunScreen Firewall for alleged disclosure of the specific types of traffic. These "alternative" obviousness arguments only serve to underscore that monitoring the specific types of traffic is not inherently disclosed by EMERALD 1997 in the first place, because they emphasize that the various prior art systems and firewalls

could monitor many different types of data for many different purposes, and that design choices would be required in order to select any particular subset of the many available options. While SRI believes that the claimed inventions are not obvious in view of these and other references because Defendants' allegations concerning the selection of the particular traffic types recited in the claims is nothing more than impermissible hindsight, there can be no question in view of the undisputed evidence here that the claimed limitations are not inherent in the disclosure of EMERALD 1997 paper alone.

V. CONCLUSION

Even assuming all the alleged facts provided in the reports and testimony of Defendants' experts are true, no reasonable jury could find clear and convincing evidence to conclude that EMERALD 1997 sufficiently describes and enables a network intrusion detection system which *necessarily*, as opposed to *possibly*, includes the limitation of monitoring and analyzing the specific types of network traffic data required by the Markush groups of the '338, '615 and '203 claims. This is particularly true where, as in this case, the prior art reference was considered by the patent examiner during prosecution. *Metabolite*, 370 F.3d at 1368. Therefore, SRI is entitled to judgment as a matter of law on the issue of no inherent anticipation. FED. R. CIV. P. 56(c).

For the foregoing reasons, SRI respectfully requests that the court grant Plaintiff's motion for partial summary judgment that the EMERALD 1997 publication does not anticipate, either expressly or inherently, any claim of the '338, '203 or '615 patent because they all require monitoring or analysis of particular types of network traffic data and such features are not disclosed expressly or inherently in that reference.

Dated: June 16, 2006

FISH & RICHARDSON P.C.

By: _____

John F. Horvath (#4557)
Kyle Wagner Compton (#4693)
FISH & RICHARDSON P.C.
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
FISH & RICHARDSON P.C.
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff/Counterclaim Defendant
SRI INTERNATIONAL, INC.

80034185.doc

CERTIFICATE OF SERVICE

I hereby certify that on June 23, 2006, I electronically filed the **PUBLIC VERSION** of **SRI INTERNATIONAL, INC.'S OPENING BRIEF IN SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT OF NO ANTICIPATION BY THE "EMERALD 1997" PUBLICATION** with the Clerk of Court the attached document using CM/ECF which will send electronic notification of such filing(s) to the following Delaware counsel.

Richard L. Horwitz
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, DE 19899

Attorneys for Defendant-Counterclaimant Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation

Richard K. Herrmann
Morris James Hitchens & Williams
PNC Bank Center
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306

Attorneys for Defendant-Counterclaimant Symantec Corporation

/s/ *John F. Horvath*
John F. Horvath

80034097.doc